

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

Absender: MIT DER INTERNATIONALEN VORLÄUFIGEN PRÜFUNG BEAUFTRAGTE BEHÖRDE

Fr. Bohdaschewskij

PCT

An:

SIEMENS AKTIENGESELLSCHAFT  
Postfach 22 16 34  
80506 München  
ALLEMAGNE

CT IPS AM Mch P

rec. SEP 15 2005

IP  
time limit 18.10.05

MITTEILUNG ÜBER DIE ÜBERSENDUNG  
DES INTERNATIONALEN VORLÄUFIGEN  
BERICHTS ZUR PATENTIERBARKEIT

(Regel 71.1 PCT)

Absendedatum  
(Tag/Monat/Jahr)

14.09.2005

Aktenzeichen des Anmelders oder Anwalts  
2003P08757WO

## WICHTIGE MITTEILUNG

Internationales Aktenzeichen  
PCT/EP2004/051153

Internationales Anmeldedatum (Tag/Monat/Jahr)  
17.06.2004

Prioritätsdatum (Tag/Monat/Jahr)  
18.06.2003

Anmelder  
SIEMENS AKTIENGESELLSCHAFT et al

1. Dem Anmelder wird mitgeteilt, daß ihm die mit der internationalen vorläufigen Prüfung beauftragte Behörde hiermit den zu der internationalen Anmeldung erstellten internationalen vorläufigen Bericht zur Patentierbarkeit, gegebenenfalls mit den dazugehörigen Anlagen, übermittelt.

2. Eine Kopie des Berichts wird - gegebenenfalls mit den dazugehörigen Anlagen - dem Internationalen Büro zur Weiterleitung an alle ausgewählten Ämter übermittelt.

3. Auf Wunsch eines ausgewählten Amtes wird das Internationale Büro eine Übersetzung des Berichts (jedoch nicht der Anlagen) ins Englische anfertigen und diesem Amt übermitteln.

### 4. ERINNERUNG

Zum Eintritt in die nationale Phase hat der Anmelder vor jedem ausgewählten Amt innerhalb von 30 Monaten ab dem Prioritätsdatum (oder in manchen Ämtern noch später) bestimmte Handlungen (Einreichung von Übersetzungen und Entrichtung nationaler Gebühren) vorzunehmen (Artikel 39 (1)) (siehe auch die durch das Internationale Büro im Formblatt PCT/IB/301 übermittelte Information).

Ist einem ausgewählten Amt eine Übersetzung der internationalen Anmeldung zu übermitteln, so muß diese Übersetzung auch Übersetzungen aller Anlagen zum internationalen vorläufigen Bericht zur Patentierbarkeit enthalten. Es ist Aufgabe des Anmelders, solche Übersetzungen anzufertigen und den betroffenen ausgewählten Ämtern direkt zuzuleiten.

Weitere Einzelheiten zu den maßgebenden Fristen und Erfordernissen der ausgewählten Ämter sind Band II des PCT-Leitfadens für Anmelder zu entnehmen.

Der Anmelder wird auf Artikel 33(5) hingewiesen, in welchem erklärt wird, daß die Kriterien für Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit, die im Artikel 33(2) bis (4) beschrieben werden, nur für die internationale vorläufige Prüfung Bedeutung haben, und daß "jeder Vertragsstaat (...) für die Entscheidung über die Patentfähigkeit der beanspruchten Erfindung in diesem Staat zusätzliche oder abweichende Merkmale aufstellen" kann (siehe auch Artikel 27(5)). Solche zusätzlichen Merkmale können z.B. Ausnahmen von der Patentierbarkeit, Erfordernisse für die Offenbarung der Erfindung sowie Klarheit und Stützung der Ansprüche betreffen.

Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde



Europäisches Patentamt  
D-80298 München  
Tel. +49 89 2399 - 0 Tx: 523656 epmu d  
Fax: +49 89 2399 - 4465

Bevollmächtigter Bediensteter

Davis, M

Tel. +49 89 2399-2703





# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT

### INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

(Kapitel II des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens)

|   |   |  |
|---|---|--|
| Aktenzeichen des Anmelders oder Anwalts<br>2003P08757WO   | <b>WEITERES VORGEHEN</b><br>siehe Formblatt PCT/IPEA/416  |  |
| Internationales Aktenzeichen<br>PCT/EP2004/051153   | Internationales Anmeldedatum (Tag/Monat/Jahr)<br>17.06.2004   | Prioritätsdatum (Tag/Monat/Jahr)<br>18.06.2003 |
| Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK<br>H04L29/06, H04L29/12, H04L12/28, H04L12/56   |   |  |
| Anmelder<br>SIEMENS AKTIENGESELLSCHAFT et al  |   |  |
| <p>1. Bei diesem Bericht handelt es sich um den internationalen vorläufigen Prüfungsbericht, der von der mit der internationalen vorläufigen Prüfung beauftragten Behörde nach Artikel 35 erstellt wurde und dem Anmelder gemäß Artikel 36 übermittelt wird.</p> <p>2. Dieser BERICHT umfaßt insgesamt 8 Blätter einschließlich dieses Deckblatts.</p> <p>3. Außerdem liegen dem Bericht ANLAGEN bei; diese umfassen</p> <p>a. <input checked="" type="checkbox"/> (an den Anmelder und das Internationale Büro gesandt) insgesamt 7 Blätter; dabei handelt es sich um</p> <p><input checked="" type="checkbox"/> Blätter mit der Beschreibung, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit Berichtigungen, denen die Behörde zugestimmt hat (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften).</p> <p><input checked="" type="checkbox"/> Blätter, die frühere Blätter ersetzen, die aber aus den in Feld Nr. 1, Punkt 4 und im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde eine Änderung enthalten, die über den Offenbarungsgehalt der internationalen Anmeldung in der ursprünglich eingereichten Fassung hinausgeht.</p> <p>b. <input type="checkbox"/> (nur an das Internationale Büro gesandt) insgesamt (bitte Art und Anzahl der/des elektronischen Datenträger(s) angeben), der/die ein Sequenzprotokoll und/oder die dazugehörigen Tabellen enthält/enthalten, nur in computerlesbarer Form, wie im Zusatzfeld betreffend das Sequenzprotokoll angegeben (siehe Abschnitt 802 der Verwaltungsvorschriften).</p> |   |  |
| <p>4. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <p><input checked="" type="checkbox"/> Feld Nr. I Grundlage des Bescheids</p> <p><input type="checkbox"/> Feld Nr. II Priorität</p> <p><input type="checkbox"/> Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit</p> <p><input type="checkbox"/> Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung</p> <p><input checked="" type="checkbox"/> Feld Nr. V Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung</p> <p><input type="checkbox"/> Feld Nr. VI Bestimmte angeführte Unterlagen</p> <p><input checked="" type="checkbox"/> Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung</p> <p><input checked="" type="checkbox"/> Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung</p>   |   |  |
| Datum der Einreichung des Antrags<br><br>15.04.2005   | Datum der Fertigstellung dieses Berichts<br><br>14.09.2005  |  |
| Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde<br><br> Europäisches Patentamt<br>D-80298 München<br>Tel. +49 89 2399 - 0 Tx: 523656 epmu d<br>Fax: +49 89 2399 - 4465   | Bevollmächtigter Bediensteter<br><br>Günther, S<br><br>Tel. +49 89 2399-6962<br><br> |  |

# INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

Internationales Aktenzeichen  
PCT/EP2004/051153

## Feld Nr. I Grundlage des Berichts

1. Hinsichtlich der **Sprache** beruht der Bericht auf der internationalen Anmeldung in der Sprache, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
  - ☐ Der Bericht beruht auf einer Übersetzung aus der Originalsprache in die folgende Sprache, bei der es sich um die Sprache der Übersetzung handelt, die für folgenden Zweck eingereicht worden ist:
    - ☐ internationale Recherche (nach Regeln 12.3 und 23.1 b))
    - ☐ Veröffentlichung der internationalen Anmeldung (nach Regel 12.4)
    - ☐ internationale vorläufige Prüfung (nach Regeln 55.2 und/oder 55.3)
2. Hinsichtlich der **Bestandteile\*** der internationalen Anmeldung beruht der Bericht auf (*Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt*):

### Beschreibung, Seiten

1-24 in der ursprünglich eingereichten Fassung  
25, 26 eingegangen am 15.04.2005 mit Schreiben vom 12.04.2005

### Ansprüche, Nr.

1-14 eingegangen am 10.08.2005 mit Schreiben vom 04.08.2005

### Zeichnungen, Blätter

1/7-7/7 in der ursprünglich eingereichten Fassung

☐ einem Sequenzprotokoll und/oder etwaigen dazugehörigen Tabellen - siehe Zusatzfeld betreffend das Sequenzprotokoll

3. ☐ Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:

- ☐ Beschreibung: Seite
- ☐ Ansprüche: Nr.
- ☐ Zeichnungen: Blatt/Abb.
- ☐ Sequenzprotokoll (*genaue Angaben*):
- ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):

4. ☒ Dieser Bericht ist ohne Berücksichtigung (von einigen) der diesem Bericht beigelegten und nachstehend aufgelisteten Änderungen erstellt worden, da diese aus den im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2 c)).

- ☐ Beschreibung: Seite
- ☒ Ansprüche: Nr. 1,12-14
- ☐ Zeichnungen: Blatt/Abb.
- ☐ Sequenzprotokoll (*genaue Angaben*):
- ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):

\* Wenn Punkt 4 zutrifft, können einige oder alle dieser Blätter mit der Bemerkung "ersetzt" versehen werden.

---

**Feld Nr. V Begründete Feststellung nach Artikel 35 (2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

---

1. Feststellung
- |                                |                            |
|--------------------------------|----------------------------|
| Neuheit (N)                    | Ja: Ansprüche 1-14         |
|                                | Nein: Ansprüche            |
| Erfinderische Tätigkeit (IS)   | Ja: Ansprüche 11           |
|                                | Nein: Ansprüche 1-10,12-14 |
| Gewerbliche Anwendbarkeit (IA) | Ja: Ansprüche: 1-14        |
|                                | Nein: Ansprüche:           |

2. Unterlagen und Erklärungen (Regel 70.7):

**siehe Beiblatt**

---

**Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung**

---

Es wurde festgestellt, daß die internationale Anmeldung nach Form oder Inhalt folgende Mängel aufweist:

**siehe Beiblatt**

---

**Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung**

---

Zur Klarheit der Patentansprüche, der Beschreibung und der Zeichnungen oder zu der Frage, ob die Ansprüche in vollem Umfang durch die Beschreibung gestützt werden, ist folgendes zu bemerken:

**siehe Beiblatt**

**Zu Punkt I**

1. Die von der Anmelderin eingereichten geänderten unabhängigen Ansprüche 1, 12, 13 und 14 bringen einen Sachverhalt ein, der im Widerspruch zu Artikel 34(2)(b) PCT über den Offenbarungsgehalt der internationalen Anmeldung im Anmeldezeitpunkt hinausgeht.

- 1.1. Zu Anspruch 1 wurde hinzugefügt, dass das internet-basierte Authentifizierungsverfahren Nachrichten "auf Basis des Internet-Protokoll Standards" übermittelt.

Diese Formulierung könnte jedoch so interpretiert werden, dass der Gegenstand von Anspruch 1 auch die Authentifikationsverfahren, die auf einer höheren Schicht über dem Internet Protokoll ablaufen, umfasst, z.B. Authentifizierung für Homebanking im Internet über ein Anwendungsprotokoll, Schicht 7.

Dies ist eine unzulässige Verallgemeinerung, da in der ursprünglichen Anmeldung nur "internet-basierte Authentifizierungsverfahren auf Schicht 3", "Extensible Authentication Protocol", "Protected Extensible Authentication Protocol", "Extensible Authentication Protocol Tunneled TLS Authentication Protocol" und "Protocol for Carrying Authentication for Network Access" (siehe Beschreibung, Seite 9, Zeilen 22-33 und Seite 11, Zeilen 10-20) enthalten sind.

- 1.2. Diese Feststellung trifft auch für die unabhängigen Ansprüche 12-14 zu.
2. Aus diesen Grund erfolgt werden anstatt der geänderten nur die ursprünglich eingereichten unabhängigen Ansprüche 1, 12, 13 und 14 geprüft.

**Zu Punkt V**

1. Es wird auf folgende Dokumente verwiesen:

D1: "Internet Key Exchange (IKEv2) Protocol", XP015002237

D2: "Internet X.509 Public Key Infrastructure", XP015002989



2. Der Gegenstand des ursprünglich eingereichten Anspruchs 1 beruht nicht auf einer erfinderischen Tätigkeit, Artikel 33(3) PCT.

2.1. Abgesehen von den Klarheitsproblemen, siehe Punkt VIII, offenbart D1 bezüglich der meisten der Merkmale von Anspruch 1 (die Verweise in Klammern beziehen sich auf dieses Dokument):

Verfahren ("IKE", Kapitel 1.2) zum Bilden einer verschlüsselten Nachricht (Seite 8, Zeilen 27-31), welche Kommunikations-Konfigurationsdaten enthält ("CP payload", Seite 31, Zeilen 14-16),

- bei dem unter Verwendung von mindestens einem Dienst einer Einheit einer Sicherungsschicht zwischen einer ersten Kommunikationseinheit und einer zweiten Kommunikationseinheit ein internet-basiertes Authentifikationsverfahren durchgeführt wird ("IKE supports ... EAP", Seite 28, Zeile 29 - Seite 29, Zeile 1),
- bei dem unter Verwendung mindestens eines kryptographischen Schlüssels ("SK\_e", Seite 8, Zeilen 27-29) die Kommunikations-Konfigurationsdaten von der ersten Kommunikationseinheit verschlüsselt werden, womit die verschlüsselte Nachricht gebildet wird ("SK {...}", Seite 8, Zeilen 27-29).

2.2. Der Gegenstand von Anspruch 1 unterscheidet sich von der Offenbarung in D1 darin, dass durch das Authentifikationsverfahren mindestens ein kryptographisches Schlüsselpaar gebildet und dass unter Verwendung mindestens eines kryptographischen Schlüssels des Schlüsselpaars verschlüsselt wird.

2.3. Das objektive technische Problem besteht in der Verstärkung des kryptographischen Schutzes für die verschlüsselten Daten.

2.4. Das Bilden eines kryptographischen Schlüsselpaars durch ein Authentifikationsverfahren und das Verwenden eines der Schlüssel dieses Schlüsselpaars zur Verschlüsselung ist eine fachübliche Massnahme, die z.B. aus D2 bekannt ist (Absätze 4.4.2 - 4.4.3.). Das Ergreifen dieser Massnahme ist z.B. durch den Hinweis auf PKIX in D1 (Seite 82, Zeilen 1-3) naheliegend.

3. Der Gegenstand der ursprünglich eingereichten unabhängigen Ansprüche 12-14 beruht nicht auf einer erfinderischen Tätigkeit, Artikel 33(3) PCT.
  - 3.1. Die meisten der Merkmale des Verfahrensanspruchs 12 entsprechen den Merkmalen des nicht erfinderischen Verfahrensanspruchs 1, und zusätzlich erwähnt Anspruch 12 noch, dass Daten unter Entschlüsselung ermittelt werden, was ebenfalls aus D1 bekannt sind (Seite 26, Zeilen 21-26). Somit gelten die Feststellungen für Anspruch 1 auch für Anspruch 12.
  - 3.2. Die Merkmale des unabhängigen Vorrichtungsanspruchs 13 entsprechen vollständig den Merkmalen des nicht erfinderischen Verfahrensanspruchs 1.
  - 3.3. Die Merkmale des unabhängigen Vorrichtungsanspruchs 14 entsprechen vollständig den Merkmalen des nicht erfinderischen Verfahrensanspruchs 12.
4. Die zusätzlichen Merkmale der abhängigen Ansprüche 2-10 fügen nichts Erfinderisches zu den unabhängigen Ansprüchen hinzu, weil diese Merkmale entweder aus dem oben zitierten Stand der Technik (Extensible Authentication Protocol, dynamisches Konfigurieren eines Endgeräts) oder als fachübliche Massnahmen (Netzwerk-Elemente, Mobilfunk-Netzwerk und -Endgeräte) bekannt sind.
5. Unter der Annahme, der Begriff "internet-basiert" im ursprünglichen Anspruch 1 wäre gemäss dem vollständigen Wortlaut in Anspruch 4 unzweifelhaft definiert, scheint unter Berücksichtigung der Argumente der Anmelderin der abhängige Anspruch 11, der auf den ursprünglichen Anspruch 1 rückbezogen ist, einen neuen und erfinderischen Gegenstand zu enthalten.
  - 5.1. D1 offenbart die meisten der Merkmale des Anspruchs 11, siehe auch 2.1.
  - 5.2. Die objektiven technischen Probleme bestehen in einer geschützten Übertragung von IP-Konfigurationsdaten zu einem Endgerät zum Zeitpunkt, wenn noch keine IP-Verbindung aufgebaut werden kann, und in der Verstärkung des kryptographischen Schutzes für die verschlüsselten Daten.

- 5.3. In Anspruch 11 werden diese Probleme gelöst, indem Kommunikations-Konfigurationsdaten gemäss einem Protokollformat eines Dynamic Host Configuration Protokolls unter Verwendung von elektronischen Nachrichten gemäss dem Authentifikationsverfahren Extensible Authentication Protocol von der ersten Kommunikationseinheit zu der zweiten Kommunikationseinheit übertragen werden, und indem ein kryptographisches Schlüsselpaar gebildet und unter Verwendung eines kryptographischen Schlüssels des Schlüsselpaars verschlüsselt wird.
- 5.4. Der nächstliegende Stand der Technik offenbart weder die vorgeschlagene Lösung noch wird diese nahegelegt. In D1 werden Konfigurationsdaten nur mittels IP-Protokoll ausgetauscht. DHCP-Konfigurationsdaten für die Zuweisung von IP-Adressen werden nicht erwähnt, und es findet sich kein Hinweis darauf, eine geschützte Übertragung von Daten ausserhalb IP vorzusehen. D2 behandelt nur die Verwendung von Zertifikaten im Umfeld einer Schlüssel-Infrastruktur für eine verstärkte Übertragungssicherheit, lässt aber DHCP-Konfigurationsdaten und Verschlüsselung ohne IP-Protokoll unerwähnt. Die verbleibenden Dokumente des Internationalen Recherchenberichts beschränken sich entweder auf gesicherte Übertragung von Konfigurationsdaten über IP, ungeschützte Übertragung von DHCP-Nachrichten oder geschützte Übertragung von Authentifizierungsdaten ohne DHCP-Nachrichten auf der Sicherungsschicht.

#### **Zu Punkt VII**

1. Die unabhängigen Ansprüche sind nicht in der zweiteiligen Form abgefaßt, Regel 6.3(b) PCT.
2. Die Merkmale der Ansprüche sind nicht mit Bezugszeichen versehen, Regel 6.2(b) PCT.

#### **Zu Punkt VIII**

1. In Anspruch 1 ist der Begriff "internet-basiert" in Zusammenhang mit



"Authentifizierungsverfahren" mehrdeutig, denn dies lässt sich als Authentifizierung über das Internet-(IP)-Protokoll, Authentifizierung mittels spezieller Internet-Standardprotokolle der IETF bzw. als Authentifizierung über das Internet-Netzwerk interpretieren, Artikel 6 PCT.

2. Der Begriff "Einheit einer Sicherungsschicht" ist in Anspruch 1 nicht definiert und kann z.B. als Bestandteil des abstrakten OSI-Schichtenmodells verstanden werden. Somit ist unklar, für welches eigentliche technische Merkmal Schutz begehrt wird, Artikel 6 PCT.
3. Die Feststellungen unter 1. und 2. gelten auch für alle anderen unabhängigen Ansprüche 12-14.

In diesem Dokument sind folgende Veröffentlichungen zitiert:

- [1] N. Prigent et al., DHCPv6 Threads, Internet-Draft, Mai 2001;
- 5
- [2] C. Schäfer, Das DHCP-Handbuch, Ein Leitfaden zur Planung, Einführung und Administration von DHCP, Edison-Wesley-Verlag, ISBN 3-8273-1904-8, Seiten 141-149, 2002;
- 10
- [3] R. Droms, Dynamic Host Configuration Protocol, Request for Comments: 2131, März 1997;
- [4] R. Droms et al., Authentication for DHCP Messages, Request for Comments : 3118, Juni 2001 ;
- 15
- [5] M. Richardson, A Method for Configuration for IPsec Clients Using DHCP, Internet-Draft, Februar 2003;
- [6] T. Kivinen, DHCP over IKE, Internet-Draft, April 2003;
- 20
- [7] D. Dukes, Configuration Payload, Internet-Draft, December 2002;
- [8] D. Dukes et al., The ISAKMP Configuration Method, Internet-Draft, September 2001,
- 25
- [9] D. Harkins et al., The Internet Key Exchange (IKE), Request for Comments: 2409, November 1998;
- 30
- [10] C. Kaufman, Internet Key Exchange (IKEv2) Protocol, Internet-Draft, April 2003;

- [11] A. McAuley et al., Dynamic Registration and Configuration Protocol (DRCP), Internet-Draft, Januar 2001;
- [12] B. Mukherjee et al., Extensions to DHCT for Roaming Users, Internet-Draft, Mai 2001;
- [13] S. Medvinsky et al., Kerberos V Authentication Mode for Uninitialized Clients, Internet-Draft, Juli 2000;
- [14] V. Gupta, Flexible Authentication for DHCP Messages, Internet-Draft, Februar 2003;
- [15] H. Tschofenig et al., EAP IKEv2 Method, Internet-Draft, April 2003;
- [16] L. Blunk et al., Extensible Authentication Protocol (EAP), Internet-Draft, Februar 2004;
- [17] D. Forsberg et al., Protocol for Carrying Authentication for Network Access (PANA), Internet-Draft, March 2003;
- [18] M. Grayson et al., EAP Authorisation, Internet-Draft, März 2003;
- [19] T. Hiller et al., A Container Type for the Extensible Authentication Protocol (EAP), Internet-Draft, Mai 2003;
- [20] H. Andersson et al., Protected EAP Protocol, Internet-Draft, Februar 2002
- [21] P. Funk, EAP Tunnel TLS Authentication Protocol (EAP-PTLS), Internet-Draft, February 2002

Patentansprüche

1. Verfahren zum Bilden einer verschlüsselten Nachricht  
(233), welche Kommunikations-Konfigurationsdaten enthält, bei  
5 dem

- unter Verwendung eines internet-basierten Authentifikati-  
onsverfahrens für eine erste Kommunikationseinheit (202)  
und eine zweite Kommunikationseinheit (201) mindestens ein  
kryptographisches Schlüsselpaar gebildet wird,

10 - als internet-basiertes Authentifikationsverfahren ein Au-  
thentifikationsverfahren eingesetzt wird, das seine Nach-  
richten auf Basis des Internet-Protokoll Standards über-  
mittelt,

- unter Verwendung mindestens eines kryptographischen  
15 Schlüssels des mindestens einen kryptographischen Schlüs-  
selpaares die Kommunikations-Konfigurationsdaten von der  
ersten Kommunikationseinheit (202) verschlüsselt werden,  
womit die verschlüsselte Nachricht gebildet wird,

dadurch gekennzeichnet, dass

20 bei den zur Übertragung zur Bildung des mindestens einen  
kryptographischen Schlüsselpaares und zur Durchführung der  
Authentifizierung zwischen der ersten und zweiten Kommunika-  
tionseinheit (201, 202) benutzten Nachrichten (205, ..., 229)  
des internet-basierten Authentifikationsverfahrens auf die  
25 Verwendung des Internet-Protokoll Standards verzichtet wird.

2. Verfahren gemäß Anspruch 1,  
bei dem das internet-basierte Authentifikationsverfahren auf  
einem Extensible Authentication Protocol-Verfahren basiert.

30

3. Verfahren gemäß Anspruch 1 oder 2,  
bei dem die Kommunikations-Konfigurationsdaten unter Verwen-  
dung von elektronischen Nachrichten gemäß dem internet-  
basierten Authentifikationsverfahren von der ersten Kommuni-  
35 kationseinheit zu der zweiten Kommunikationseinheit übertra-  
gen werden.

4. Verfahren gemäß einem der Ansprüche 1 bis 3,  
bei dem die Kommunikations-Konfigurationsdaten unter Verwen-  
dung von elektronischen Nachrichten gemäß einem der folgenden  
internet-basierten Authentifikationsverfahren von der ersten  
5 Kommunikationseinheit zu der zweiten Kommunikationseinheit  
übertragen werden:

- Protected Extensible Authentication Protocol-Verfahren,
- Extensible Authentication Protocol Tunneled TLS Authenti-  
10 cation Protocol-Verfahren, oder
- Protocol for Carrying Authentication for Network Access-  
Verfahren.

5. Verfahren gemäß einem der Ansprüche 1 bis 4,  
bei dem die erste Kommunikationseinheit eine Kommunikations-  
15 einheit eines Kommunikationsnetzwerk-Elements ist.

6. Verfahren gemäß Anspruch 5,  
bei dem die erste Kommunikationseinheit eine Kommunika-  
tions-  
einheit eines Kommunikationsnetzwerk-Elements in einem Mobil-  
20 funk-Kommunikationsnetzwerks ist.

7. Verfahren gemäß einem der Ansprüche 1 bis 6,  
bei dem die zweite Kommunikationseinheit ein Kommunikations-  
endgerät ist.

25 8. Verfahren gemäß Anspruch 7,  
bei dem die zweite Kommunikationseinheit ein Mobilfunk-  
Kommunikationsendgerät ist.

30 9. Verfahren gemäß einem der Ansprüche 1 bis 8,  
bei dem die Kommunikations-Konfigurationsdaten gemäß einem  
Protokollformat eines Protokolls zum Konfigurieren eines Kom-  
munikationsendgeräts codiert sind.

35 10. Verfahren gemäß Anspruch 9,



bei dem die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Protokolls zum dynamischen Konfigurieren eines Kommunikationsendgeräts codiert sind.

5 11. Verfahren gemäß Anspruch 10,  
bei dem die Kommunikations-Konfigurationsdaten gemäß einem Protokollformat eines Dynamic Host Configuration Protokolls zum dynamischen Konfigurieren eines Kommunikationsendgeräts codiert sind.

10

12. Verfahren zum Entschlüsseln einer verschlüsselten Nachricht (233), welche Kommunikations-Konfigurationsdaten enthält, bei dem

- 15 - unter Verwendung eines internet-basierten Authentifikationsverfahrens für eine erste Kommunikationseinheit (202) und eine zweite Kommunikationseinheit (201) mindestens ein kryptographisches Schlüsselpaar gebildet wird,
- als internet-basiertes Authentifikationsverfahren ein Authentifikationsverfahren eingesetzt wird, das seine Nachrichten auf Basis des Internet-Protokoll Standards über-
- 20 mittelt,
- unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaares die Kommunikations-Konfigurationsdaten von der
- 25 zweiten Kommunikationseinheit (201) unter Entschlüsselung der verschlüsselten Nachricht (233), welche die Kommunikations-Konfigurationsdaten enthält, ermittelt werden,

dadurch gekennzeichnet, dass

30 bei den zur Übertragung zur Bildung des mindestens einen kryptographischen Schlüsselpaares und zur Durchführung der Authentifizierung zwischen der ersten und zweiten Kommunikationseinheit (201, 202) benutzten Nachrichten (205, ..., 229) des internet-basierten Authentifikationsverfahrens auf die Verwendung des Internet-Protokoll Standards verzichtet wird.

35

13. Einrichtung zum Bilden einer verschlüsselten Nachricht (233), wobei die verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält,

- mit einer Schlüsselerzeugungs-Einheit, welche eingerichtet ist, mit einem internet-basierten Authentifikationsverfahrens für eine erste Kommunikationseinheit (202) und eine zweite Kommunikationseinheit (201) mindestens ein kryptographisches Schlüsselpaar gebildet wird, wobei als internet-basiertes Authentifikationsverfahren ein Authentifikationsverfahren eingesetzt wird, das seine Nachrichten auf Basis des Internet-Protokoll Standards übermittelt, wobei bei den zur Übertragung zur Bildung des mindestens einen kryptographischen Schlüsselpaares und zur Durchführung der Authentifizierung zwischen der ersten und zweiten Kommunikationseinheit (201, 202) benutzten Nachrichten (205, ..., 229) des internet-basierten Authentifikationsverfahrens auf die Verwendung des Internet-Protokoll Standards verzichtet wird,
- mit einer Verschlüsselungseinheit, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaares die Kommunikations-Konfigurationsdaten zu verschlüsseln, womit die verschlüsselte Nachricht gebildet wird.

14. Einrichtung zum Entschlüsseln einer verschlüsselten Nachricht (233), wobei die verschlüsselte Nachricht Kommunikations-Konfigurationsdaten enthält,

- mit einer Schlüsselerzeugungs-Einheit, welche eingerichtet ist, mit einem internet-basierten Authentifikationsverfahrens für eine erste Kommunikationseinheit (202) und eine zweite Kommunikationseinheit (201) mindestens ein kryptographisches Schlüsselpaar gebildet wird, wobei als internet-basiertes Authentifikationsverfahren ein Authentifikationsverfahren eingesetzt wird, das seine Nachrichten auf Basis des Internet-Protokoll Standards übermittelt, wobei bei den zur Übertragung zur Bildung des

mindestens einen kryptographischen Schlüsselpaares und zur Durchführung der Authentifizierung zwischen der ersten und zweiten Kommunikationseinheit (201, 202) benutzten Nachrichten (205, ..., 229) des internet-basierten Authentifikationsverfahrens auf die Verwendung des Internet-Protokoll Standards verzichtet wird,

- mit einer Entschlüsselungseinheit, welche eingerichtet ist, unter Verwendung mindestens eines kryptographischen Schlüssels des mindestens einen kryptographischen Schlüsselpaars Kommunikations-Konfigurationsdaten von der zweiten Kommunikationseinheit (201) unter Entschlüsselung der verschlüsselten Nachricht (233), welche die Kommunikations-Konfigurationsdaten enthält, zu entschlüsseln.